WHITE PAPER

DIGITAL GUARDIAN®

DIGITAL GUARDIAN FOR APPLICATION WHITELISTING

Technology Overview

WHAT IT IS

Most of the application whitelisting products on the market today are too difficult to deploy, time-consuming to manage, and vulnerable to a single point of failure. Our application whitelisting is easy to deploy, transparent to existing operations and the most secure application whitelisting for Retail POS systems and industrial control systems.

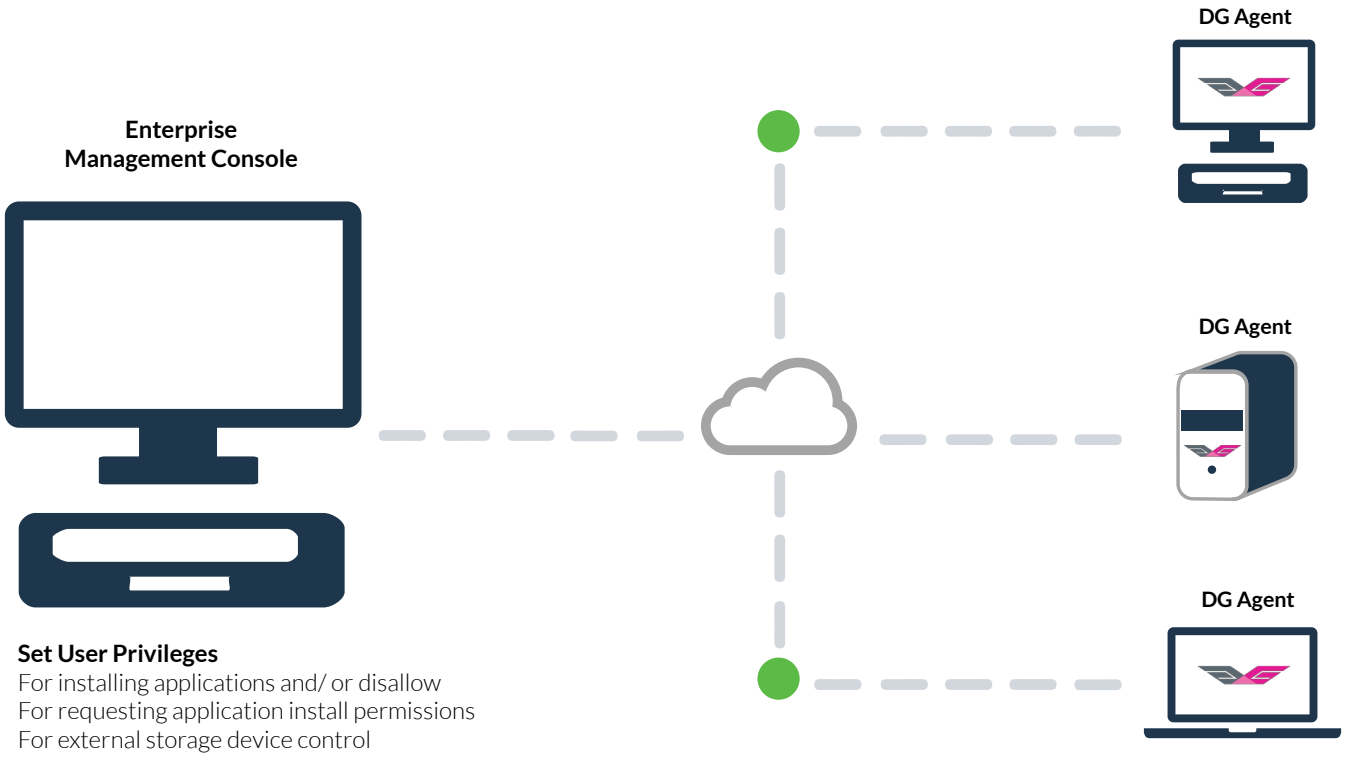
INNOVATIVE ARCHITECTURE

DG Application Whitelisting is based on a patented client-centric architecture that is fundamentally different from the approach of other application whitelisting vendors and **does not depend on a large centralized database.**

DG Application Whitelisting has two software components:

1. A lightweight agent that is installed on each endpoint that an organization wants to protect and manage. The agent is also fully secure and operational when disconnected from the console.

2. A web-based management console that runs on IIS and Apache internet servers and enables centralized management and reporting on the application-related activities on the endpoints on which the agents are installed. The client-centric architecture ensures high performance and enables easy integration with other IT infrastructure.



Set User Privileges
For installing applications and/ or disallow
For requesting application install permissions
For external storage device control

Configure Trusted Updaters and Processes
Interact seamlessly with provisioning and patching
Flexible update methods

Set Log and Alert Methods and Parameters
Approved installs
Authorized user installs
Blocked applications including malaware

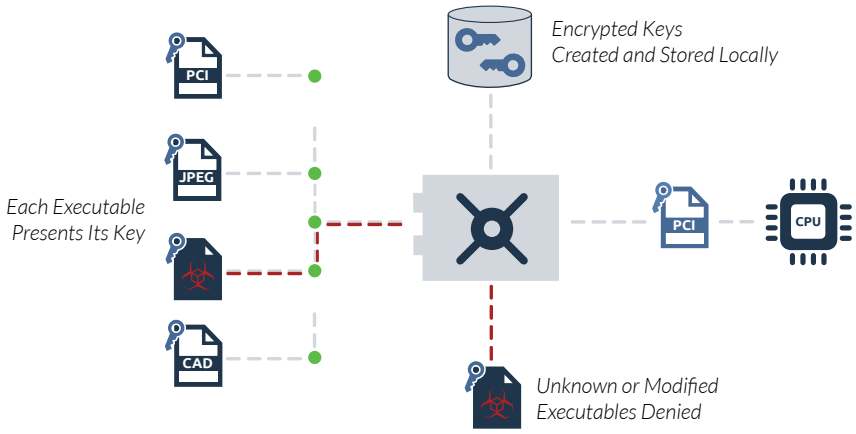
Deploy the Agent
And automatically protect existing executable (auto–whitelist)

Dynamically enforces, protects, enable, tracks
Enforces user policy
Protects from unauthorized executables
Enables trusted changes and processes
Logs changes made and blocks unauthorized attempts

HOW IT WORKS

DG Application Whitelisting software associates a unique, invisible key with each authorized application (including associated components and identified scripts) on each end system. When an executable file is read or accessed, our agent compares the previously known key with the key that is presented. If there is a match, the application is allowed to execute on the system. If there is not a match or the application is unknown, access to the file is denied and it cannot execute. In lockdown mode, new executable files are prevented from even being written to disc. In a more open environment where users may be granted more flexibility in adding software to their devices, options are presented for handling the unknown application.

System administrators can use their existing remote management and/or patching procedures to install or update applications on end devices. Our management console provides the ability to manage the set-up, configuration and permissions for any device through a simple web interface. However, unlike other whitelisting solutions, ours does not require a central application key store. The keys themselves are stored in an encrypted database on the local system which is accessible only by the DG software. This eliminates the need to query a central server or reference database, improves system performance, and eliminates a central point of attack.



WHY IT MATTERS

DG Application Whitelisting operates effectively in static environments in which endpoint software does not change frequently or need to be updated often, such as with industrial automation and POS devices. Our software also works effectively in dynamic environments in which applications change frequently or users are allowed to independently add software to their computers.

EASY INITIAL DEPLOYMENT

Our agents install in minutes and begins protecting endpoint systems immediately. Our software does not require administrators to determine in advance which applications and libraries are required by each user. Immediately after being installed on an endpoint, the agent automatically creates a unique whitelist that determines what executables are permitted to run on that device. It scans the system drives to identify existing executables. For each executable it identifies, the agent generates a key that is unique to both the file and the end point. The keys are encrypted and stored in a local database on the endpoint. After creation of the initial whitelist, any new executable that does not have a key assigned to it for that device cannot execute. The initial whitelist is updated continually to include new authorized software and authorized updates to software on the initial list.

Note: DG agents are best deployed after IT has scanned, updated and patched systems to ensure that the initial whitelist is based on a machine that is compliant with security policies.

SIMPLER ONGOING OPERATION

Since it does not depend on software signatures and continuous updates from centralized databases and does not need to query a central server or reference database, managing and using our solution is much simpler than other application whitelisting products. Once it is operational it prevents new unauthorized applications from being installed. Upon confirmation of the approved whitelist, execution of any unauthorized application will be blocked, whether malicious applications (such as viruses, Trojans, or Bots) or unwanted/unknown applications. Digital Guardian operates independently of Windows administrator mode so even a user with Windows administrator privileges cannot override the agent.

ENABLES AUTOMATIC CHANGES

Through the designation of trusted agents, DG Application Whitelisting enables you to use your normal methods for patching, updating and installing software without having to explicitly look at or manage a white list, thereby minimizing IT overhead. Examples of agents that IT administrators might designate as trusted agents include Windows update, antivirus, endpoint management software, patching software and self-updating software such as such as Adobe Acrobat Reader, and desktop configuration agents. Our trusted agent feature allows you to efficiently keep all authorized applications on endpoints updated and patched without requiring any additional intervention by the endpoint user or IT personnel.

AUTOMATIC CONTAINMENT

If pre-existing malware or malicious code was undetected by scans and antivirus prior to the installation and creation of the initial whitelist, Digital Guardian will automatically contain any potential negative effects from the presence of that malware only to that device. Even if malware on the whitelist of one device moves to a second device on which our agent is also installed, the malware will not be able to execute on the second device because the keys assigned to that malware on the first device will not have a match in the encrypted database on the second device. This automatic containment capability harnesses our patented unique whitelist database, providing unprecedented protection against advanced persistent threats.

COMPREHENSIVE MANAGEMENT CAPABILITIES

Using our simple web interface, you can:

- Centrally control and manage configuration and permissions for all agent endpoints.
- Have centralized visibility to events and activity logged by agents on the endpoints.

Enables Automatic Updates from Endpoint Management System
Trusts all changes made by RMM agent
Trusts SW provisioned by agent
Includes patches and updates

Automatic updates directly from trusted sources
Software can be updated automatically & directly from the ISVs
Transparent to user

Complements Antivirus
AV software updates automatically
Signature updates are automatic and trusted
Scans allowed - but cannot change files

The central console enables IT administrators to enforce corporate policies in a granular manner across the entire enterprise, such as by setting policies by users, groups, servers, and devices.

Customers can use the central management capabilities for a range of other functions beyond configuring endpoints and logging events. Other functions include endpoint application inventory, system information, and storage device (USB) control. Large organizations and MSPs tend to already have endpoint management systems and therefore value the policy enforcement and security capabilities. SMBs, on the other hand, are less likely to have an endpoint management product and frequently use the full range of our management capabilities.

MINIMAL IMPACT ON SYSTEM RESOURCES

The agent typically uses 15-30 MB of memory, and CPU usage is negligible during normal operation. It does not need to update, download, or scan lists of known signatures. The only times the client uses any additional CPU time is when new files are being authorized (such as when a program applies updates to itself and the agent is authorizing those changes as they occur).

PLATFORMS SUPPORTED

- Windows 8
- Windows Server 2012
- Windows 7
- Windows Server 2008 R2
- Windows Vista – SP1 or greater
- Windows XP – SP3 – .NET Framework version 2.0, 3.0 or 3.5 must be installed
- Windows Server 2003 – SP1 or greater
- Enterprise Management System runs on Apache/MySQL or IIS/MSSQL
- Both 32 and 64 bit versions of the above OSs
- Embedded versions of the above OSs

ABOUT DIGITAL GUARDIAN

Digital Guardian is the only data aware security platform designed to stop data theft. The Digital Guardian platform performs across traditional endpoints, mobile devices and cloud applications to make it easier to see and stop all threats to sensitive data. For more than 10 years we've enabled data-rich organizations to protect their most valuable assets with an on premise deployment or an outsourced managed security program (MSP). Our unique data awareness and transformative endpoint visibility, combined with behavioral threat detection and response, let you protect data without slowing the pace of your business.

DIGITAL GUARDIAN®
Formerly VERDASYS

CORPORATE HEADQUARTERS
860 Winter Street, Suite 3
Waltham, MA 02451 USA
info@digitalguardian.com
781-788-8180
www.digitalguardian.com

SHARE